(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2003 (05.06.2003)

PCT

(10) International Publication Number
WO 03/046819 A1

(51) International Patent Classification[7]: G06K 9/78, 9/68

(21) International Application Number: PCT/AU02/01579

(22) International Filing Date:
25 November 2002 (25.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PR 9121 26 November 2001 (26.11.2001) AU

(71) Applicant *(for all designated States except US)*: **ARGUS SOLUTIONS PTY LTD** [AU/AU]; Level 10, 55 Lavender Street, Milsons Point, NSW 2061 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SMITH, Craig, Gregory** [AU/AU]; 93 Yarrara Road, West Pymble, NSW 2073 (AU). **GRIMES, John, Andrew** [AU/AU]; 34 Anderson Street, Chifley, ACT 2600 (AU).

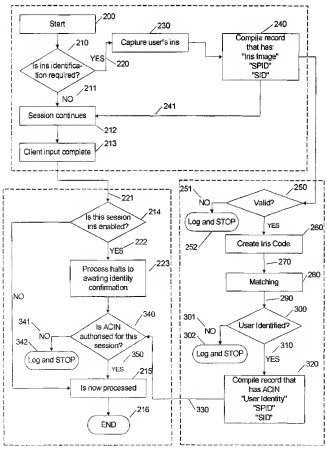
(74) Agent: **F B RICE & CO**; 605 Darling Street, Balmain, NSW 2041 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: COMPUTERISED IDENTITY MATCHING MANAGEMENT



(57) Abstract: The invention concerns a computerized identity matching management process. The process comprises the steps of a management computer receiving a request from capture apparatus waiting to commence a biometric capture process, to initiate the capture process. The management computer responds to the request to return a message to the capture apparatus at a first instant in time, the message containing a unique code, and where receipt of the message containing the code at the capture apparatus causes initiation of the capture process. The management computer, after returning a message, receives a captured biometric from the capture apparatus coded with the code, at a second instant in time. The management computer operates, when the second instant is less than a predetermined time later than the first instant, to decode the captured biometric and initiate a matching process to find a match for the decoded captured biometric against stored records and to generate an identification code when a match is found. The invention further concerns a computerized identity matching management unit, and an electronic message.

WO 03/046819 A1

European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

Computerised Identity Matching Management

Technical Field

This invention concerns computerised identity matching management. Identity matching can be performed in a number of ways. The invention is concerned with managing the provision of identity matching services to enable users to gain appropriate access to various facilities or services. This invention is provided in a number of different species. First it is provided as a process, then it is provided as a unit and system. It is also provided as essential messages.

Background Art

The iris is formed by a process of chaotic morphogenesis, which means that its final structure is randomly derived. As a result every eye is different. Even identical twins, or clones for that matter, have a unique iris in each eye. Iris scans can therefore be used to produce a biometric which will accurately identify individuals. The outlier population – those unable to use iris recognition due to eye or iris damage - is less than 2%, the smallest outlier population of any biometric.

The concept of iris recognition was developed and patented by Iridian Technologies Inc, and their concept patent US 4,641,349 describes the use of the iris to identify individuals. US 5, 291, 560 describes a method by which a biometric, including the iris pattern of an individual, can be used as the basis of an identification technique.

Briefly, the Iridian technology involves the use of an appropriate camera designed to photograph the iris of an individual user. Proprietary software associated with the camera captures the iris image and checks it is of suitable quality and that it has sufficient iris content to match successfully. This software is designed to operate only for a predetermined time after image capture commences, and the process has to be restarted if a suitable image is not obtained within that time period.

An authentication server stores as records iriscodes which are templates derived from iris images. Each record is stored with an associated customer ID number. When the server receives an image from the software, it confirms image integrity before initiating a recognition process by comparing the received iriscode with the stored iriscode records. When a match is made the

server is able to issue the customer ID number of the matched record to a service provider. The match may be verification (1:1 matching) or identification (1:many matching).

The service provider is then able to access its own records to determine the identity of the individual from the customer ID number and allocate rights to that individual accordingly - for instance access rights, or rights to conduct predetermined types of transactions.

Disclosure of Invention

In a first aspect, the invention is a computerised identity matching management process, comprising the steps of:

a management computer receiving a request, from capture apparatus waiting to commence a biometric capture process, to initiate the capture process;

the management computer responding to the request to return a message to the capture apparatus at a first instant in time, the message containing a unique code, and where receipt of the message containing the code at the capture apparatus causes initiation of the capture process;

the management computer, after returning a message, receiving a captured biometric from the capture apparatus coded with the code, at a second instant in time; and

the management computer operating, when the second instant is less than a predetermined time later than the first instant, to decode the captured biometric and initiate a matching process to find a match for the decoded captured biometric against stored records and to generate an identification code when a match is found.

The essence of the invention is the time limit imposed on the period between the issue of the unique code which initiates the capture process, and the receipt of the biometric coded with the code. The same code is only ever issued once. This time limit is determined according to the time required for the capture process, and serves to reduce the possibility of the introduction of a false biometric. For instance a time limit of ninety seconds has been found to be suitable when an iris biometric is to be captured.

In a second aspect, the invention is a computerized identity matching management unit, comprising:

a management computer programmed to receive a request, from capture apparatus waiting to commence a biometric capture process, to initiate the capture process.

The computer is also programmed to respond to the request to return a message to the capture apparatus at a first instant in time, the message containing a unique code, and where receipt of the message containing the code at the capture apparatus causes initiation of the capture process.

The computer is also programmed to receive a captured biometric coded with the code at a second instant in time, after the first instant.

The computer further being programmed, when the second instant is less than a predetermined time later than the first instant, to decode the captured biometric and initiate a matching process to find a match for the biometric against stored records and to generate an identification code when a match is found.

The management computer will typically sit on a message oriented middleware (MOM) platform. The middleware platform may comprise of e-business infrastructure products such as those provided by TIBCO ActiveEnterprise. In particular TIB/Rendezvous, TIB/Adapter and TIB/Hawk. This facilitates secure and transparent communications between capture apparatus, such as an Iridian camera installation where a user has an iris biometric captured, an authentication server together with its own secure database, also available from Iridian, where matching takes place, and a service provider's computer system which holds records of users and their access rights.

A network of distributed management computers could be employed with the nearest computer being used for each identity check. This allows for load sharing, redundancy and minimization of network latency. Of course, the management computer could be combined with an authentication server. It may also be incorporated into the service provider's computer system if required. In this case networked further computers could be made available for off-site redundancy.

In a third aspect, the invention is a computerized identity matching management system, comprising the unit in combination with an authentication server to perform the matching process to find a match for the biometric against stored records and to generate an identification code when a match is found.

The system may also be incorporated with a service providers computer system.

The management computer need hold no personal or account details of the users. It may receive no data other than any identity information provided by the user in using the identity matching process, or routed back from the authentication computer to the service provider. As a result, users do not risk their privacy when having their identity checked. In fact the management computer provides a privacy protection layer for both user and service provider.

In addition, the management computer separates the identity matching process from the subsequent application run between the user and the service provider. The only link being any information provided by the user when using the identity matching process.

In a more detailed identity matching process, the user may access the service provider's website, and then launch a client program of the management computer resident on the website. The client sends a request to the management computer for a 'message authentication code', and the management computer responds by sending a unique code having a predetermined time proscription.

At the website the client receives the code and initiates the Iridian proprietary software to capture an image of the user's iris. The captured image may be encrypted, compressed and coded with the message authentication code. It is then packed with any required identifiers and sent back to the management computer.

The management computer receives the package, checks it for validity, in particular whether the code is still valid. It also checks for integrity. It is decompressed and decrypted and the image is then passed to an authentication server for matching. The image may be directly matched, or a template may be generated from it, say by using the Daugman Algorithm, and the template matched.

If the match is made, an identifier is retrieved from the authentication server and provided to the service provider. The service provider looks up its own records using the identifier to determine who the user is and what access or transaction rights they are to be allowed.

Two applications currently exist in Australia for the management computer, AKITA (formerly iService) and GIDDiY. There are also bespoke applications which will support the management computer.

In a fourth aspect the invention is an electronic message for transmission by a management computer during a computerized identity matching process to biometric capture apparatus after the management computer has received a request, from the capture apparatus, to initiate the capture process; the electronic message comprising a unique code. Receipt of the message at the capture apparatus causes initiation of the capture process.

In a fifth aspect the invention is a second electronic message for transmission by a biometric capture apparatus during a computerized identity matching process to a management computer after the capture process has been completed. The second electronic message comprising a captured image coded with the unique code obtained from the management computer.

Brief Description of Drawings

An example of the system will now be described with reference to the accompanying drawings; in which:

Fig. 1 is a schematic diagram of a computerized identity matching management system and its working environment; and

Fig. 2 is a flow chart showing the operation of a computerized identity matching management process.

Best Modes for Carrying Out the Invention

Fig. 1 is an overview of the elements required to perform a computerized identity matching management process. At the heart of the elements is a management computer 20 programmed to receive and transmit messages through a firewall 30 and over the Internet 40 to client software 50. The client software 50 may reside in a laptop 60 or PC 70 for personal use, on a network 80 for access by many users, or on any application with processor dependent functions. In any event, the client software 50 works together with Iridian PrivateID software 90 and an Iridian Technologies iris recognition camera 100, such as the (Panasonic) Authenticam. (The process of supporting an identification management function is not restricted to biometric interfaces, nor is it restricted to the KnoWho Authentication Server(KWAS)). The Authenticam™ video camera is specifically designed for use in iris recognition. Its features include:

- A specialized lens to photograph the iris.
- A base that rests on the user's computer or monitor.

- A USB connection to the user's computer.
- An auxiliary lens to support standard video-conferencing applications.
- Safety – meeting the appropriate requirements for a consumer camera.

The management computer 20 will typically sit on a middleware platform 130. The middleware platform 130 comprises e-business infrastructure products such as those provided by TIBCO ActiveEnterprise. In particular TIB/Rendezvous, TIB/Adapter and TIB/Hawk.

TIB/Rendezvous provides the following benefits:

- Subject-based addressing (network details are hidden).
- Allows for fast application development.
- Provides platform independence at the hardware, operating system, network configuration and protocol levels.
- Component processes can be removed, replaced or added without downtime.
- Applications can scale easily.
- Location transparency.
- Provides anonymous communication between clients/hosts.
- Transparent coexistence with other communications protocols on the same computers and networks.
- Low overheads, C library size <100kB, programs in the vicinity of 64kB, communications executable daemon of 100kB.
- Is thread safe, multiple processor safe.
- Supports Multicast addressing.
- Distributed licensing.

TIB/Adapter is built so as to connect the Iridian KnoWho Authentication Server 140 to the TIB. The TIB/Iridian Adapter allows a "no-coding" approach to integration with the TIB.

TIB/Hawk is a tool for monitoring and managing distributed applications and systems within a network. System administrators can use it to monitor application parameters, behavior and loading for all nodes, and take action when pre-defined conditions occur. Using it, runtime failures can be repaired automatically within seconds of their discovery, reducing downtime.

The Iridian Technologies KnoWho Authentication Server 140 accepts the iris image sent from a camera, confirms the image integrity, and then sends it through the iris recognition process for verification against records stored in its cache, which in turn is drawn from the secure database 150. Verification may

involve 1:1 matching or 1:many identification, depending upon the strategy needed by the service provider's Transaction Application.

The database 150 stores three types of biometric information with the Subject's ID number:

- iriscode templates (left or right eye or both) in cache and on disk
- Iris images (left or right eye or both) on disk – optional. Is used for re-enrolment purposes
- Portrait images (JPEGs of a VGA image, ~ 20 KB) on disk – optional.

The KnoWho Authentication Server does not store personal data, but does index each iriscode template with a customer ID number (CIN), preserving privacy. The iriscode record is not available to the client that communicates the iris image.

The customer ID is then forwarded to the service provider 120 back through the middleware platform 130 and a firewall 160.

When a user 110 wishes to access the services of a service provider 120, they launch the service provider's website and/or application and start a session 200, as shown in Fig. 2.

The website requires session based identification (could be transaction based identification) and requests the user to select to use a conventional username/password, or the biometric identification service 210.

In the event that the user selects conventional identification 211, the session may continue 212 in a conventional fashion. The client input is completed 213, the service provider session is not enabled for biometric identity matching 214 and the session is able to be processed 215 to its conclusion 216 - none of which is of interest to this example of the invention.

In the event that the biometric identification service is selected 220, the client software 50 is launched and captures the Iridian PrivateID software 90 to take control of the video camera 100. The client also puts the session on hold.

Then the client software 50 sends a request to management computer 20 for a Message Authentication Code (MAC).

The management computer 20 responds to the client request and issues a MAC. The MAC has variable time validity and is unique (i.e.: is only ever issued once).

The client software 50 receives the MAC and the PrivateID 90 processes commence to capture an iris image.

To use the Authenticam camera 100 the user 110 moves their head so that the eye being photographed is 43 – 48cm (17 to 19 inches) from the lens. The video camera sends images to the software running on the user's laptop. The Authenticam camera responds to a software power-on command. Then an image capture module is launched.

The PrivateID software captures a series of digital video images of the Subject's eye. Image quality metrics within the PrivateID software inspect the images for sufficient quality and iris content to ensure high confidence for a successful match outcome. Once a satisfactory image has been culled 230, the software provides an audible signal to inform the user that the image capture session is complete, this usually issues within seconds. If a satisfactory image cannot be captured within the allotted time (the default is set at 10 seconds), then the software provides an error signal to the Transaction Application. The Subject would then have to restart the process.

The client software 50 encrypts the captured image using an appropriate cryptographic algorithm. Then it compresses the captured image, codes the compressed image using the previously issued MAC, collects a pre-determined session identifier (SID) and service provider identifier (SPID) and assembles a message 240 for transmission to the management computer 20.

The client also provides a message 241 to allow the transaction to continue, and the service provider is enabled for biometric identity matching 222. The service provider then waits 223.

The management computer receives the message and checks it for validity using MAC, that is to ensure it has been received while the MAC is still valid 250. If it is not valid 251 then the process stops 252.

The message then has its integrity checked using a checksum, and is decompressed and decrypted. It is then passed through a Daugman Algorithm, or similar, to create an iriscode 260.

The iriscode is then sent 270, via the middleware 130, to the authentication server 140 which attempts to match it 280 with a record in its secure database 150. The authentication server returns a result 290. The management computer interprets the result 300. If the result is a comparison failure 301, that result is logged and the process stops 302.

If the match is a success 310 the management computer receives the Customer Identification Number (ACIN) associated with the matched record back from the authentication server 140, via the middleware layer 130.

The management computer then assembles a message 320 containing the Customer Identification Number (ACIN) and the session identifier (SID), and sends this 330 to the service provider 120, via a second firewall 160, using the service provider identifier (SPID) to address it.

The service provider 120 has been enabled to receive a biometric identification signal and responds to the message from the management computer 20 by checking 340 whether the session identifier (SID) and Customer Identification Number (ACIN) are appropriate for the session or not. It does this by checking its own database to determine the rights available to the user having the ACIN found from matching. If that user does not have the appropriate rights for the session 341 the event is logged and the session ended 342.

In the event the customer has the right to conduct that session 350, they are permitted to proceed with the session transactions 215, and when they are finished the session ends 216.

Although Fig.1 shows the management computer running at a single facility, in reality there would be multiple facilities for load sharing, redundancy and minimization of network latency.

Although the invention has been described with reference to a particular example it should be appreciated that it may be operated in other ways. For instance, a Turnkey solution may alternatively be provided where a service provider houses the management computer on their own premises together with an AKITA application. Here the individual transactions of an application could require user identity matching before they can be performed. In this case transaction identifiers are sent to the management computer with the coded images, rather than session identifiers.

In a Guaranteed Identification Do it Yourself (GIDDiY), the users create their own 'customer identification numbers' (ACINs), independent of third parties, and store them at trusted locations.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A computerised identity matching management process, comprising the steps of:

a management computer receiving a request, from capture apparatus waiting to commence a biometric capture process, to initiate the capture process;

the management computer responding to the request to return a message to the capture apparatus at a first instant in time, the message containing a unique code, and where receipt of the message containing the code at the capture apparatus causes initiation of the capture process;

the management computer, after returning a message, receiving a captured biometric from the capture apparatus coded with the code, at a second instant in time; and

the management computer operating, when the second instant is less than a predetermined time later than the first instant, to decode the captured biometric and initiate a matching process to find a match for the decoded captured biometric against stored records and to generate an identification code when a match is found.

2. A process according to claim 1, wherein the predetermined time is determined according to the time required for the biometric capture process.

3. A process according to claim 1 or claim 2, wherein the management computer further operates to check the integrity of the decoded biometric.

4. A process according to any one of the preceding claims, wherein the matching process includes generating a template image of the decoded captured biometric for matching against stored records.

5. A process according to any one of the preceding claims, further comprising the step of providing the identification code to a service provider for comparison against a second set of stored records.

6. A computerized identity matching management unit, comprising:

a management computer programmed to:

receive a request, from capture apparatus waiting to commence a biometric capture process, to initiate the capture process;

respond to the request to return a message to the capture apparatus at a first instant in time, the message containing a unique code, and where receipt of the message containing the code at the capture apparatus causes initiation of the capture process;

receive a captured biometric coded with the code at a second instant in time, after the first instant; and

when the second instant is less than a predetermined time later than the first instant, to decode the captured biometric and initiate a matching process to find a match for the biometric against stored records and to generate an identification code when a match is found.

7. A management unit according to claim 6, further comprising a network of distributed management computers.

8. A management unit according to claim 6 or 7, further comprising a privacy protection layer between the management computer and at least the capture apparatus.

9. A management unit according to any one of claims 6 to 8, further comprising a message oriented middleware platform in communication with the, or each, management computer for facilitating secure communication between the management computers and at least the capture apparatus.

10. A computerised identity matching management system, comprising the management unit in accordance with any one of claims 6 to 9 in combination with an authentication server to perform the matching process to find a match for the biometric against stored records and to generate an identification code when a match is found.

11. A management system according to claim 10, wherein the system is incorporated with a service providers computer system.

12. A management system according to claim 10 or claim 11, wherein the management computer only receives identity information data provided by a

user when using the identity matching process and/or data routed back from the authentication server to a service provider such that the user does not risk their privacy when having their identity checked.

13. An electronic message for transmission by a management computer during a computerised identity matching process to biometric capture apparatus after the management computer has received a request, from the capture apparatus, to initiate the capture process; wherein the electronic message comprising a unique code and wherein receipt of the message at the capture apparatus causes initiation of the capture process.

14. An electronic message for transmission by a biometric capture apparatus during a computerised identity matching process to a management computer after receipt of the message of claim 13, and after the capture process has been completed, wherein the electronic message comprises a captured image coded with a unique code obtained from the management computer.

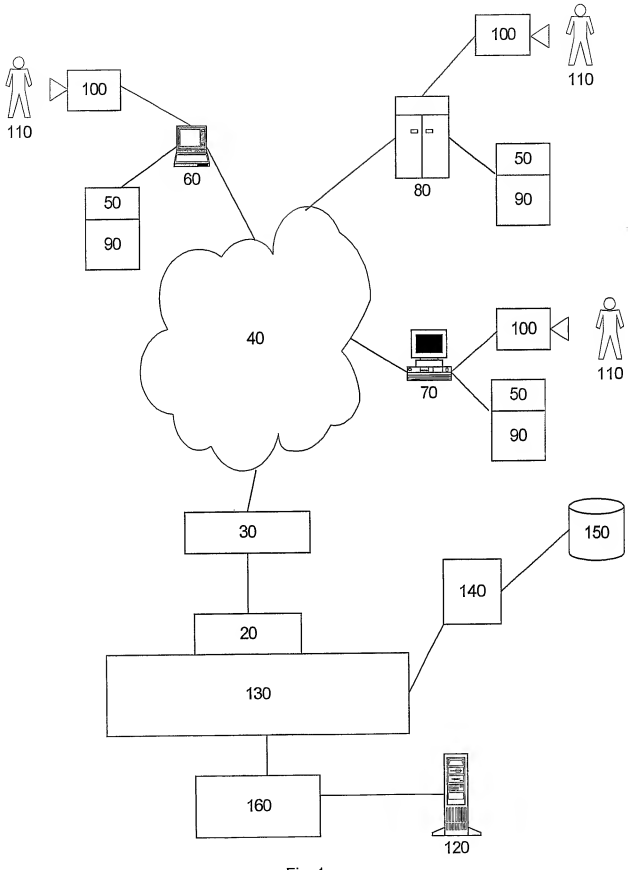

100
110
100
110
60
80
50
90
50
90
40
100
110
70
50
90
30
150
140
20
130
160
120

Fig. 1

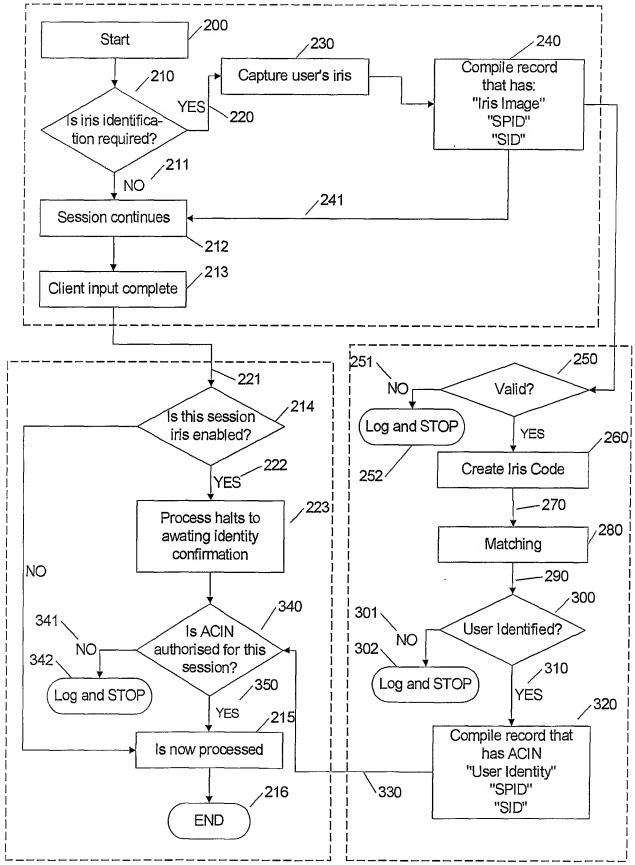

Start
200
Capture user's iris
230
Compile record that has: "Iris Image" "SPID" "SID"
240
210
Is iris identification required?
YES
220
NO
211
Session continues
241
212
Client input complete
213
221
Is this session iris enabled?
214
YES
222
Process halts to awating identity confirmation
223
NO
341
Is ACIN authorised for this session?
340
NO
342
Log and STOP
350
YES
215
Is now processed
216
END
251
NO
Valid?
250
Log and STOP
YES
252
260
Create Iris Code
270
Matching
280
290
301
User Identified?
300
NO
302
Log and STOP
310
YES
320
Compile record that has ACIN "User Identity" "SPID" "SID"
330

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU02/01579

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06K 9/78 G06K 9/68

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT. G06K 9/- and keywords: iris, code, time and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/68873 A (AUTHENTEC, INC.) 16 November 2000 page 13, lines 10-16; claims 25-26	1-14
A	US 6307955 A (ZANK et al.) 23 October 2001 column 2, line 16 - column 3, line 19	1-14
A	EP 973122 A (MEDIA TECHNOLOGY CORP.) 19 January 2000 whole document	1-14

☐ Further documents are listed in the continuation of Box C

☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2002	16 DEC 2002
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**ROSEMARY LONGSTAFF** Telephone No : (02) 6283 2637

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU02/01579

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
WO	200068873	AU	200050003	EP	1183638
US	6307955	NONE			
EP	973122	JP	2000036036		

END OF ANNEX